Status

No claim has been added or cancelled. Independent claims 1 and 24 with attendant claims depending therefrom will remain for further consideration.

More Clearly Defined

The claims in this application have been revised to voluntarily further clarify Applicant's unique invention. Applicant maintains that the claims as filed were patentable over the art of record. However, to expedite issuance of this application, reconsideration of the claims in light of the amendments and for the following reasons is respectfully requested.

Claim History

The Examiner rejected claims 1-10, 13, 14, 17-21, 23-31, 34, 36, 38-42. 44-54, 57 59, 61-65, 67 under 35 U.S.C. § 102 as being anticipated by Kara. The Examiner rejected claims 11, 12, 14, 16, 22, 32, 33, 35, 37, 43, 55, 56, 58, 60, 66 under 35 U.S.C. § 103 over Kara.

35 U.S.C. § 102

The Examiner rejected claims 1-10, 13, 14, 17-21, 23-31, 34, 36, 38-42. 44-54, 57 59, 61-65, 67 under 35 U.S.C. § 102 as being anticipated by Kara.

DRAWINGS

Formal Drawings

Formal drawings were filed with the application on 6/21/2001. A review of the Office Action has failed to uncover whether the drawings were accepted by the Official Draftsman or whether a Form 948 rejection was issued by the Official Draftsman. An indication of the status of the drawings is respectfully requested with the next communication from the Patent Office.

The patent to Kara shows a system that ensures the "accuracy" of a document from its origination to delivery. It does not provide the security features and especially security combined with accuracy. Kara shows a program for sending a public key encrypted document and a cipher ("bit count or random bits from the document") to a "certification" program. The program merely checks the checksum or summary count and the document and verifies the document by the checksum count or cipher, presumably by making its own checksum calculation or generating its own cipher. If there is a match, a certificate is issued certifying the content of the message. To do this, the certification computer must have its own copies of the private decryption key ("MK" or "Message Key").

The encrypted document and cipher are then sent to recipient along with the decryption key ("MK"). The entire process can only be as secure as the e-mail system which it is run on. Thus there is no additional security provided by the Kara system to the e-mail system since the encryption provides no security as long as the decryption key is provided attached to the document.

In any case, there is no provision for separate sender and recipient keys so that a document can be sent WITHOUT an attached private key ("decryption key") and without the sender and user needing the key of the other party. The OC acts as a clearing house for the purpose of facilitating the transmission of information between two parties without the parties having to contact each other to obtain each other's keys and without having to divulge their own keys, especially their private keys. This is the opposite of Kara and is not taught or suggested by Kara. Kara only verifies to the recipient that the document is

the true document, it does not verify to the sender that the recipient is the anticipated party.

Claim 1 as amended shows a clearing house for e-mail that receives an e-mail from a sender and authenticates the sender using the key system. The OC then establishes a secure connection with the sender to receive the document to be delivered. The OC then authenticates the recipient and sends the encrypted document to the recipient. The entire trail of the document is auditable and secure. As shown in the dependent clauses, further messages and tracking details can be sent to the OC to complete the audit trail when the parties use the OC as an auditor and facilitator but not a transmission means. None of this is shown, anticipated or taught by Kara.

Likewise, claim 24 shows a first key associated with the sender and a second key associated with the recipient for communicating with the clearing house ("OC") to transfer messages. Kara merely uses the encryption key to make forgery more difficult, not to secure the transfer of files since the decryption key is provided along with the encrypted file.

As to claim 6, Applicant respectfully submits that Figure 3B nowhere anticipates a virtual private network as recited. The figure does not show any other than a "communication" with a second site.

For the reasons discussed above, the Applicant respectfully submits that the claims are allowable over the art of record and that this case is ready to be passed to issue.

35 U.S.C. §103

The Examiner rejected claims 11, 12, 14, 16, 22, 32, 33, 35, 37, 43, 55, 56, 58, 60, 66 under 35 U.S.C. §103 over Kara.

Each of these claims depends from an independent claim discussed above. None of the showings argued by the Examiner cure the defects described above in Kara. Therefore, the Applicant respectfully submits that the claims are allowable over the art of record and that this case is ready to be passed to issue for at least the same reasons as the independent claims 1 and 24 discussed above.

Summary

Applicants have made a diligent and bona fide effort to answer each and every ground for rejection or objection to the specification including the claims and to place the application in condition for final disposition. Reconsideration and further examination is respectfully requested, and for the foregoing reasons, Applicant respectfully submits that this application is in condition to be passed to issue and such action is earnestly solicited. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Robert N. Blackmon, Applicants' Attorney at 703-684-5633 to satisfactorily conclude the prosecution of this application.

Dated: May 24, 2005

Respectfully submitted,

Robert N. Blackmon
Reg. No. 39494
Attorney/Agent for Applicant(s)

Merek, Blackmon & Voorhees, LLC
673 S. Washington St.
Alexandria, Virginia 22314
Tel. 703-684-5633
Fax. 703-684-5637
E-mail: RNB@ BlackmonLaw.com